Чернадчук Т.О.,
кандидат юридичних наук, доцент,
доцент кафедри адміністративного і інформаційного права
Сумського національного аграрного університету

УДК 342.951
DOI https://doi.org/10.32845/2663-5666.2021.1.9

ДО ПИТАННЯ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ У СФЕРІ ПРОТИДІЇ ЗАГРОЗІ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ КРАЇНИ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

Постановка проблеми. Європейські прагнення і європейський вибір України покладає на неї зобов'язання розбудовувати демократичну й економічно розвинуту сталу державу. Так, у країні впроваджуються політичні, соціально-економічні, правові та інституційні реформи, значне місце серед яких посідає розбудова інформаційного суспільства. Проведення реформи інформатизації надає широкі можливості для сучасної України в напрямі створення цифрової держави, зокрема й формування та реалізації державної політики у сфері цифрової економіки, цифрових інновацій, електронного урядування, розвитку інформаційного суспільства. Існування інформаційного суспільства тісно пов'язане з розвитком інформаційних технологій та використанням інтернет-мережі у всіх сферах життєдіяльності. За даними Організації Об'єднаних Націй, крадіжка інформації під час проведення фінансових операцій через інтернет-мережу є найпоширенішим злочином із використанням інформаційних технологій.

До того ж в умовах поширення організованої злочинності, що має транскордонний характер, виникає гостра потреба в належному забезпеченні інформаційної безпеки України – базового складника національної безпеки. Належний стан інформаційної безпеки вимагає вжиття дієвих заходів, що направлені на боротьбу з наявними та латентними загрозами, однією з яких є кіберзлочинність. Сьогодні в Україні, за інформацією Департаменту кіберполіції, кількість кіберзлочинів, які вчиняються за допомогою комп'ютерних технологій та ІТ щороку зростає. Найбільш поширеним є розповсюдження комп'ютерних вірусів, крадіжки грошей із банківських рахунків, викрадення інформації, онлайн-торгівля наркотиками та зброєю, формування у дітей суїцидальної поведінки (смертельна гра «Синій кит» 2017 р.; «Зникнути на 24 години» – гра, під час якої зникали діти в різних країнах світу; нова гра 2020 р. «Виклик стрибка», наслідком якої може стати струс мозку або й смерть). Варто також згадати про наслідки дії вірусу «Petya» («NotPetya»), у результаті чого була дестабілізована робота інформаційних систем Секретаріату Кабінету міністрів України, Міністерства внутрішніх справ України, Державної фіскальної служби України, Національного банку України, підприємств «Укртелеком», «Епіцентр», «Київенерго», «WOG», «Нова пошта», «Ощадбанк», Чорнобильської атомної електростанції та багатьох інших [1], що, очевидно, призвело до мільярдних збитків і завдало шкоди національній економіці.

Відповідно, сьогодні існує проблема одночасного забезпечення інформаційної безпеки України та боротьби з кіберзлочинністю, яка загрожує інформаційній безпеці.

Аналіз останніх досліджень і публікацій. Останнім часом окремі аспекти проблеми кіберзлочинності як загрози інформаційній безпеці перебувають у сфері інтересів науковців і практиків. Вони знайшли своє відображення у працях таких учених, як М.В. Гуцалюк, М.О. Кравцова, В.В. Марков, Є.Д. Скулиш, О.В. Таволжанський та ін. Незважаючи на це, все ще існує потреба в її подальшому дослідженні, що, на наш погляд, дозволить надати цілісне уявлення щодо окресленої проблематики.

Мета статті – на підставі аналізу наукових праць, міжнародно-правових актів, національного законодавства розкрити сутність кіберзлочинності, яка становить загрозу інформаційній безпеці України, з подальшим визначенням оптимальних шляхів боротьби з цим негативним явищем.

Виклад основного матеріалу. На сучасному етапі розвитку людського суспільства важливим стратегічним ресурсом, що потребує охорони, є інформація, яка містить надзвичайно широкий спектр зведень (від простих даних про громадян країни до стратегічних державних програм). Тому ці дані все частіше стають предметом зло-

чинних зазіхань. Комплексне і широкомасштабне використання інформаційних технологій на основі персональних комп'ютерів, інформаційно-обчислювальних мереж і комп'ютеризованих комунікаційних систем забезпечило людству вихід на новий етап свого розвитку – етап інформаційного суспільства. Наслідком цього є поява нового виду злочинності – комп'ютерної, або кіберзлочинності [2, с. 108].

За оперативною інформацією Держспецзв'язку щодо захисту державних інформаційних ресурсів, тільки за період із 30 грудня 2020 року до 05 січня 2021 року Система захищеного доступу державних органів до інтернет-мережі заблокувала 76 328 атак різних видів. Система кіберзахисту державних інформаційних ресурсів та об'єктів критичної інфраструктури за той же період на об'єктах моніторингу зафіксувала 5 055 047 підозрілих подій, більшість із яких стосуються спроб викрадення інформації (38%), мережевого сканування (27%), спроб отримання прав користувача (13%) та адміністратора (12%) [3]. Тому в умовах сьогодення боротьба з кіберзлочинністю – одна з найактуальніших проблем в усьому світі, де поряд із невпинним розвитком і вдосконаленням інформаційно-комунікативних технологій створюються нові схеми та методи заволодіння чужими коштами та здійснюється доступ до певних персональних даних, що спричиняє виникнення чергових загроз інформаційній безпеці кожної країни.

Кіберзлочинність як загрозу інформаційній безпеці розглядають чимало вчених. Так, Ю.І. Хлапонін, С.В. Кондакова та інші під час дослідження тенденцій кіберзлочинності зазначають, що остання є загрозою інформаційній безпеці країни, де використання сучасних інформаційних технологій (і в державних структурах, і в суспільстві в цілому) включає вирішення проблем інформаційної безпеки до групи основних [4, с. 6]. Я.Я. Пушак й О.М. Марченко також розглядають кіберзлочинність як загрозу інформаційній безпеці, адже науково-технічний прогрес у сфері інформаційних технологій призводить до зростання небезпеки втрати та викрадення інформації через технічні засоби її обробки [5, с. 173].

Потреба в забезпеченні інформаційної безпеки зумовлюється такими факторами, як необхідність підтримки національної безпеки, створення надійного інформаційного простору, а також потреба в протидії будь-яким інформаційним загрозам, що можуть завдати шкоду як інтересам окремого суб'єкта, так і держави загалом. Із зазначеного зрозуміло, що кіберзлочинність є однією із загроз інформаційній безпеці країни, яка є складником національної безпеки.

Про те, що кіберзлочинність є загрозою інформаційній безпеці, свідчить також низка міжнародних і національних актів законодавства, де серед міжнародних актів важливе місце посідає Конвенція про кіберзлочинність (Будапештська конвенція). Її ухвалення обґрунтовувалося тим, що під час злочинної діяльності зловмисники все частіше вдаються до використання електронних систем обробки даних та впливають на їх роботу, тому потребує вирішення питання про злочини, вчинені проти і за допомогою електронних мереж. Указана Конвенція залишається найвпливовішою міжнародною угодою, що регулює питання порушення закону через інтернет-мережу або інші інформаційні мережі. Вона вимагає від сторін модернізації і гармонізації свого кримінального законодавства проти дій хакерів та інших порушень безпеки, включаючи порушення авторських прав, шахрайство за допомогою комп'ютера, дитячу порнографію та іншу протиправну кібердіяльність [6, с. 160–161]. Ця Конвенція була ратифікована Україною ще у 2005 році, що означає, що вже тоді держава розуміла потенційні загрози, які можуть виникати у результаті вчинення кіберзлочинів.

Правову основу вітчизняного законодавства у сфері кібернетичної безпеки становлять: Конституція України, Кримінальний кодекс України, закони України «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про основні засади забезпечення кібербезпеки України», «Про національну безпеку України», укази Президента України «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України», «Про Національний координаційний центр кібербезпеки», «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року, «Про Доктрину інформаційної безпеки України». Така кількість актів українського законодавства підтверджує важливість і необхідність боротьби з кіберзлочинністю.

Розглядаючи кіберзлочинність як загрозу інформаційній безпеці країни, зауважимо, що термін «кіберзлочинність» визначено та закріплено Законом України «Про основні засади забезпечення кібербезпеки України», згідно з яким кіберзлочинність – це сукупність кіберзлочинів. Водночас кіберзлочин (комп'ю-

терний злочин) – суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України [7].

На доктринальному ж рівні у широкому значенні під кіберзлочинністю розуміють усі види злочинів, у яких використовуються сучасні телекомунікаційні мережі, в яких комп'ютери або комп'ютерні мережі використовуються для злочинної діяльності [8]. М.О. Кравцова та О.М. Литвинов визначають кіберзлочинність як соціально-правовий феномен, що виявляється в забороненій законом про кримінальну відповідальність предметній діяльності (кримінальній активності) частини населення з використанням електронно-обчислювальних машин (комп'ютерів), телекомунікаційних систем, комп'ютерних мереж і мереж електрозв'язку [9, с. 19].

Щодо видів кіберзлочинів, то їх умовно поділяють на 4 види (відповідно до Конвенції про кіберзлочинність):

1) правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем;

2) правопорушення, пов'язані з комп'ютерами;

3) правопорушення, пов'язані зі змістом (контентом), що полягає у здійсненні умисних незаконних дій щодо вироблення, пропонування або надання доступу, розповсюдження дитячої порнографії, а також володіння такими файлами у своїй системі;

4) умисні дії, пов'язані з порушенням авторських та суміжних прав, відповідно до вимог Бернської Конвенції про захист літературних і художніх творів, Угоди про торговельні аспекти прав інтелектуальної власності та Угоди Всесвітньої організації інтелектуальної власності про авторське право, а також національного законодавства України [10].

Кіберзлочини, на противагу традиційним, мають низку характерних особливостей, серед яких виділяють такі:

1) місце вчинення кіберзлочину може перебувати в різних юрисдикціях: правопорушник активізує кібератаку, наприклад, з інтернет-кафе однієї країни, бот-мережа перебуває в другій, а атакована інформаційна система – у третій;

2) переважна кількість доказів кіберзлочинів існують в електронній формі (так звані «електронні» («цифрові») докази). Вони можуть швидко знищуватися чи модифікуватися;

3) внаслідок специфічної природи кіберпростору постраждалий не завжди обізнаний про вчинення кіберзлочину [11, с. 119];

4) злочини у сфері інформаційного права щодо використання комп'ютерних технологій та телекомунікацій належать до таких, склад яких (а іноді і сам факт скоєння) довести надзвичайно важко, тоді як подібні діяння можуть завдавати значної шкоди як корпоративним, так і особистим майновим і немайновим інтересам [12, с. 90].

Водночас поширенню кіберзлочинності сприяють такі чинники: процеси глобалізації світової економіки; гіперпопит на різні види інформаційних послуг у розвинутих країнах світу; розвиток сучасних інформаційних технологій, особливо інтернет-ресурсів, що забезпечують майже неконтрольований процес формування спокус [13, с. 161]. Поширенню саме організованості кіберзлочинності в сучасних умовах сприяють два взаємопов'язані складники: по-перше, організована злочинність намагається використовувати кіберпростір у своїх цілях, по-друге, складний характер кіберзлочинів змушує осіб, які спеціалізуються на вчиненні злочинів у мережевому інформаційному просторі, координувати свої дії, об'єднуватися і створювати організовані кримінальні співтовариства [11, с. 120].

Ураховуючи вищезазначене, для України особливо актуальним є питання боротьби з кіберзлочинністю, відповідальність за яку передбачено в окремому розділі Кримінального кодексу України, що присвячений злочинам у сфері використання електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 361 – 363-1). Також до групи кіберзлочинів належать ст. 176 (порушення авторського права і суміжних прав), ст. 190 (шахрайство) та ст. 301 (ввезення, виготовлення, збут і розповсюдження порнографічних предметів) [14].

Сьогодні окремими науковцями висловлюється думка щодо потреби в посиленні боротьби з кіберзлочинністю. Так, М.В. Гуцалюк пропонує посилити санкції за вчинення злочинів, передбачені статтями 361, 361-1, 361-2, 362, 363, 363-1 Кримінального кодексу України, що дасть змогу перевести їх у розряд тяжких злочинів, посилить кримінальну відповідальність за їх вчинення, а також розширить перелік негласних слідчих (розшукових) заходів, що можуть бути проведені для їх припинення або документування [11, с. 127]. Ця пропозиція є цілком

слушною, зважаючи на наслідки, до яких може призводити кіберзлочинність.

Обґрунтовуючи доцільність посилення кримінальної відповідальності за кіберзлочини, звернемося до думки Є.Д. Скулиша, який причини посилення відповідальності вбачає в особливих рисах, що притаманні подібним злочинам, які й зумовлюють потребу в застосуванні до винних осіб більш суворих заходів впливу:

1) негативні наслідки кіберзлочинів найчастіше виявляються не одразу, а лише з часом (у процесі реалізації суспільних відносин);

2) особи, які скоюють кіберзлочини, характеризуються неординарними розумовими здібностями, які в поєднанні з девіантною поведінкою можуть призводити до появи нових негативних суспільних явищ, що несе в собі суттєві ризики для користувачів інформації;

3) об'єктом кіберзлочинів часто є специфічна інформація, яка стосується сфери національної інформаційної безпеки. Це може зумовлювати негативні наслідки кіберзлочинів уже не на корпоративному чи приватному, а на публічному державному рівні. Протиправне заволодіння такою інформацією та її подальше поширення призводить і до більш масштабних негативних наслідків – загрози національній безпеці держави [12, с. 95–96].

Водночас в Україні на законодавчому рівні вже були спроби посилити кримінальну відповідальність за кіберзлочини, що передбачалося законопроектами, один із яких було зареєстровано ще у 2015 році, а інший – у 2018 році. Так, останнім законопроектом за № 8304 [15] пропонувалося розмежувати підслідність кіберзлочинів і посилити відповідальність. Наприклад, несанкціоноване втручання в роботу об'єктів критичної інформаційної інфраструктури має становити 6–8 років, а не 2–5 років, а збут і розповсюдження шкідливих програм має каратися штрафом 3–5 тисяч неоподатковуваних мінімумів доходів громадян замість 0,5–1 тисячі. Таке покарання є досить справедливим й співмірним із вчиненими діяннями та наслідками, до яких призвели такі діяння. Однак цей законопроект так і не був ухвалений, зважаючи на виявлені в ньому недоліки та висловлені зауваження.

Як засвідчує досвід інших держав, посилення кримінальної відповідальності за кіберзлочини є світовою тенденцією, що знайшла своє виправдання, адже досі жодна держава не переглянула питання щодо пом'якшення відповідальності за вказані злочини.

Наприклад, однією з перших країн, що вжила заходів щодо встановлення кримінальної відповідальності, стала Америка, санкції за шахрайство з використанням комп'ютерів, несанкціонований доступ до інформації урядового відомства та інші злочини за § 1030(a) Титулу 18 Зводу законів США становлять до 10 років тюремного ув'язнення, а у разі рецидиву – до 20 років [16]. Також за останні 3 роки питання про посилання кримінальної відповідальності розглядали Росія й Узбекистан.

Ураховуючи те, що в умовах глобалізації інформаційного обміну, широкого використання ІТ проблема безпеки у кіберпросторі стає однією з ключових, із метою гарантування високого рівня кібербезпеки у всіх сферах життєдіяльності суспільства спеціальні органи держави укладають між собою угоди. Так, наприклад, Національний координаційний центр кібербезпеки Ради національної безпеки і оборони України та Антимонопольний комітет України уклали Меморандум про взаємодію та співробітництво у сфері кібербезпеки та кіберзахисту, «Укренерго» підписало меморандум із РНБО України в згаданій сфері та ін. На міжнародному рівні (відповідно до укладених двосторонніх і багатосторонніх договорів з іноземними державами, міжнародними організаціями) Україна здійснює співробітництво у сфері кібербезпеки. Прикладом може слугувати підписаний 12 вересня 2019 року Меморандум про взаємодію та співробітництво у сфері кібербезпеки та кіберзахисту між Міжнародною фундацією виборчих систем (IFES)/IFES Україна та Державним центром кіберзахисту Державної служби спеціального зв'язку та захисту інформації України.

Як зазначалося вище, найбільше від кіберзлочинності потерпає фінансовий сектор економіки держави, особливо банківська сфера. З метою протидії актуальним загрозам від кіберзлочинів на вимогу Закону України «Про основні засади забезпечення кібербезпеки України» в структурі Національного банку України був створений Центр кіберзахисту НБУ. У серпні 2019 року між ним і Державним центром кіберзахисту Державної служби спеціального зв'язку та захисту інформації був підписаний Меморандум про взаємодію та співробітництво у сфері кібербезпеки та кіберзахисту, направлений на попередження, виявлення, своєчасне та ефективне реагування, протидію кіберзагрозам.

При цьому зазначимо: незважаючи на значні кроки у сфері протидії кіберзлочинності, загро-

за інформаційній безпеці держави і, відповідно, національній безпеці України залишається актуальною.

Висновки. Підсумовуючи наведені міркування, слід констатувати, що сьогодні кіберзлочинність є суттєвою загрозою інформаційній безпеці України. Кіберзагроза ж зумовлена розвитком і поширенням інформаційно-комунікаційних технологій і організованої злочинності. Особливостями кіберзлочинів є їх латентність, необмеженість у часі та просторі, можливість використання механізму шифрування даних, автоматизований режим, зважаючи на що, актуальним питанням є боротьба з кіберзлочинністю. Нагальним залишається посилення кримінальної відповідальності. Втім, на нашу думку, для комплексної боротьби з кіберзлочинністю нарівні зі змінами до кримінального законодавства потрібно: гармонізувати вітчизняне кримінальне законодавство про кіберзлочинність із міжнародним, що позитивно вплине на стан протидії та боротьби з кіберзлочинністю; якнайшвидше імплементувати положення Конвенції про кіберзлочинність у частині призначення органу, який би цілодобово приймав заяви та повідомлення про кіберзлочини та надавав негайну допомогу для розслідування або переслідування щодо цих кримінальних правопорушень; налагодити взаємодію вітчизняних правоохоронних органів із правоохоронними органами інших країн, що є особливо актуальним, зважаючи на транскордонний характер кіберзлочинів і поширення організованої кіберзлочинності; вдосконалити обмін інформацію правоохоронних органів між собою й із суб'єктами банківської системи, адже більшість кіберзлочинів учиняються саме в банківській сфері.

Таким чином, ураховуючи негативні наслідки від кіберзлочинності та світові тенденції, важливим сьогодні залишається подальше вдосконалення основних напрямів боротьби з нею. На наш погляд, це значно підвищить ефективність і результативність боротьби з указаними злочинами, а також сприятиме захищеності інформаційної безпеки, особливо в умовах розвитку інформаційного суспільства і цифрової держави.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. В Україні десятки компаній та установ атакував комп'ютерний вірус. URL: https://hromadske.ua/posts/ukrposhtu-ukrenerho-ta-banky-atakuvav-podibnyi-do-wannacry-virus.

2. Марков В.В. До питання щодо зарубіжного досвіду протидії кіберзлочинності. *Право і безпека*. 2015. № 2 (57). С. 107–113.

3. Захист державних інформаційних ресурсів України 30.12.2020 – 05.01.2021. URL : https://cip.gov.ua/ua/news/operativna-informaciya-derzhspeczv-yazku-shodo-zakhistu-derzhavnikh-informaciinikh-resursiv-za-period-z-30-grudnya-2020-po-05-sichnya-2021-roku

4. Хлапонін Ю.І., Кондакова С.В., Шабала Є.Є., Юрчук Л.П., Демяечук П.С. Аналіз стану кібербезпеки в провідних країнах світу. *Кібербезпека: освіта, наука, техніка*. 2019. Вип. 4. Т. 4. С. 6–13.

5. Пушак Я.Я., Марченко О.М. Проблемні аспекти запобігання та протидії кіберзлочинності в Україні. *Економічна та інформаційна безпека: проблеми та перспективи*: матер. Міжнар. наук.-практ. конф. (м. Дніпро, 27 квітня 2018 р.). Дніпро, 2018. С. 173–176.

6. Посібник з європейського права у сфері захисту персональних даних. Київ : К.І.С., 2015. 216 с.

7. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовтня 2017 р. № 2163-VIII. URL : https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення 12.01.2021).

8. Rush H., Smith C., Kraemer-Mbula, E., Tang, P. Crime online: cybercrime and illegal innovation. London, UK: NESTA, 2009. URL: https://cris.brighton.ac.uk/ws/portalfiles/portal/206133/Crime_Online.pdf.

9. Кравцова М.О., Литвинов О.М. Запобігання кіберзлочинності в Україні. Харків : Панов, 2016. 210 с.

10. Нікулеско Д. Кібербезпека: вразливі моменти. *Юридична газета online*. 2019. URL: https://yur-gazeta.com/publications/practice/inshe/kiberbezpeka-vrazlivi-momenti.html

11. Гуцалюк М.В. Сучасні тенденції організованої кіберзлочинності. *Інформація і право*. 2019. № 1 (28). С. 118–128.

12. Скулиш Є.Д. Посилення відповідальності в контексті підвищення ефективності боротьби із кіберзлочинністю. *Правова інформатика*. 2013. № 4 (40). С. 90–97.

13. Таволжанський О.В. Особливості забезпечення кібербезпеки у сучасному світі: огляд суб'єктів запобігання кіберзлочинності. *Науково-інформаційний вісник Івано-Франківського університету права імені Короля Данила Галицького. Серія Право*. 2018. № 6 (18). С. 154–163.

14. Кримінальний кодекс України : Закон України від 5 квітня 2001 р. № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14#n2506 (дата звернення 12.01.2021).

15. Проект Закону про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо розмежування підслідності злочинів, вчинених у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, державних інформаційних ресурсів і об'єктів критичної інформаційної інфраструктури від 19 квітня 2018 р. № 8304. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=63907

16. Evdokimov K. N. Comparative legal analysis of the legislation of Russia and foreign countries, regulating the criminal liability for committing computer crimes. *Science and Society.* 2016. № 3. V. 1. Pp. 104–121.

Чернадчук Т.О. ДО ПИТАННЯ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ У СФЕРІ ПРОТИДІЇ ЗАГРОЗІ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ КРАЇНИ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

Статтю присвячено розкриттю сутності кіберзлочинності, яка становить загрозу інформаційній безпеці України, з подальшим визначенням оптимальних шляхів боротьби з цим негативним явищем. Актуальність описаної в статті проблеми зумовлена особливостями кіберзлочинів і поширенням транскордонної організованої злочинності. У статті обґрунтована потреба у забезпеченні інформаційної безпеки, що зумовлено відповідними факторами. Узагальнено міжнародні та національні акти, що становлять правову основу боротьби з кіберзлочинами. Розкрито поняття «кіберзлочинність» на законодавчому та доктринальному рівнях, види кіберзлочинів, їх характерні особливості на противагу традиційним злочинам, а також чинники поширення кіберзлочинності та організованої кіберзлочинності. Зроблено акцент на потребі в посиленні боротьби з кіберзлочинністю шляхом посилення кримінальної відповідальності та обґрунтовано доцільність посилення кримінальної відповідальності за кіберзлочини. Проаналізовано спроби українського законодавця посилити кримінальну відповідальність за вказані злочини. Зауважено, що посилення кримінальної відповідальності за кіберзлочини є світовою тенденцією, про що свідчить досвід окремих країн.

Звернено увагу на те, що найбільше від кіберзлочинності потерпає фінансовий сектор економіки держави, особливо банківська сфера. Саме крадіжка інформації під час проведення фінансових операцій через інтернет-мережу є найпоширенішим злочином з використанням інформаційних технологій. Незважаючи на низку заходів, вжитих в Україні з метою протидії актуальним загрозам від кіберзлочинів у згаданій сфері, як-от створення в структурі Національного банку України Центру кіберзахисту НБУ, питання протидії кіберзлочинності залишається актуальним. Зазначено, що, окрім посилення кримінальної відповідальності, для комплексної боротьби з кіберзлочинністю потрібно вжити й інших заходів, зокрема й гармонізувати вітчизняне кримінальне законодавство про кіберзлочинність із міжнародним, імплементувати окремі положення Конвенції про кіберзлочинність, налагодити взаємодію вітчизняних правоохоронних органів із правоохоронними органами інших країн, удосконалити обмін інформацію правоохоронних органів між собою та суб'єктами банківської системи.

Ключові слова: інформаційна безпека, кіберзлочини, кіберзлочинність, кримінальна відповідальність, організована злочинність, цифрова держава.

Chernadchuk T.O. AS FOR THE QUESTION OF FIGHTING WITH CIBERCRIME IN THE SPHERE OF COUNTERACTION OF THE STATE INFORMATIVE SECURITY THREAT IN THE DIGITAL TRANSFORMATION CONDITIONS.

The article deals with the disclosure of the essence of cybercrime, which poses a threat to the information security of Ukraine, with further determination of the optimal ways of combating this negative phenomenon. The urgency of the problem described in the article is caused by the peculiarities of cybercrime and the spread of cross-border organized crime. The article substantiates the need for information security, which is due to the relevant factors. Generalized are the international and national acts that make up the legal basis for combating cybercrime. The concept of "cybercrime" at the legislative and doctrinal levels, types of cybercrime, their characteristic features as opposed to traditional crimes, as well as the factors of spread of cybercrime and organized cybercrime are revealed. Emphasis is placed on the need to strengthen the fight against cybercrime by enhancing criminal responsibility and substantiate the feasibility of enhancing criminal liability for cybercrime. Attempts by the Ukrainian legislator to strengthen criminal liability for these crimes are analyzed. It is noted that increasing criminal liability for cybercrime is a worldwide trend, as evidenced by the experience of individual countries. Attention is drawn to the fact that the financial sector of the state's economy and especially the banking sector suffer the most from cybercrime. Theft of information during financial transactions via the Internet is the most common crime in the world using information technology. Despite a number of measures taken in Ukraine to counter the current threats of cybercrime in this area, such as the establishment of the National Bank of Ukraine Center for Cyber Defense of the NBU, the issue of combating cybercrime remains relevant. It is noted that in addition to strengthening criminal responsibility, for the integrated fight against cybercrime it is necessary to take other measures, in particular to harmonize domestic criminal legislation on cybercrime with international law, to implement certain provisions of the Convention on cybercrime, to establish interaction of national authorities with domestic law enforcement agencies among themselves and with the subjects of the banking system.

Key words: information security, computer crime, cybercrime, criminal responsibility, organized crime, digital state.